Judicial Evidence Integrity and Security System for Proof of Fair Judgement

**Abstract**

Digital evidence is defined as information and data of value to an investigation that is stored on, received, or transmitted by an electronic device. In criminal investigations, civil lawsuits, and regulatory compliance, digital evidence such as electronic documents, recordings, and transaction records forms the basis for decision-making. However, factors like data alteration, unauthorised access, or flaws in centralised storage can threaten the security and integrity of digital evidence. Therefore, a secure storage model is needed to improve the investigation process and safeguard any sensitive information collected. To address the lack of an automated mechanism for preserving evidence and maintaining integrity, a model was developed targeting the various security and forensic aspects during the investigation lifecycle. An efficient forensics architecture is proposed that establishes the Chain of Custody (CoC) in blockchain technology and tamper detection using Deep Learning Models, where participating stakeholders create a private network to exchange and agree on different investigation activities before being stored on the blockchain ledger. Detecting tampering in various types of files using deep learning algorithms are Image with CNN, Word Document Embedding’s using BERT, Video Frame-level Analysis with TCN, Audio Spectrogram Analysis with CNN, PDF Document Structure Analysis. Utilizing fuzzy hash functions enables forensic investigators to successfully deal with permissible alteration of digital evidence by standardizing the forensics processes, DB-CoC architecture enforcing a standard approach and improves the quality of the finished result. The proposed architectural solution delivers robust information integrity, prevention, and preservation mechanism to permanently and immutably store the evidence (chain of custody) in a private permissioned encrypted blockchain ledger. The proposed DB-CoC architecture provides complete data provenance, traceability, and assurance for performing different operations as well as trust between the chain of custody events while collecting, storing, analysing, and interpreting the digital evidence.